In the Specification:

Rewrite the paragraph at page 1, lines 19-21, as follows:

The present invention relates to wireless communication systems, such as cellular systems and PCS systems, and more particularly relates to methods ~~and systems for reducing theft of wireless telephony services by~~ involving use of steganographically encoded ~~authentication~~ data in conjunction with such systems.

JB

Rewrite the paragraph at page 3, lines ~~7~~ 3-12, as follows:

To overcome this failing, ~~the preferred embodiments of the present invention~~ one embodiment steganographically encodes the voice signal with identification data, resulting in "in-band" signaling (in-band both temporally and spectrally). This approach allows the carrier to monitor the user's voice signal and decode the identification data therefrom.

Rewrite the paragraph extending between page 3, line 18 and page 4, line 5, as follows:

In ~~the preferred form of the invention~~ certain embodiments, the steganographic encoding relies on a pseudo random data signal to transform the message or identification data into a low level noise-like signal superimposed on the subscriber's digitized voice signal. This pseudo random data signal is known, or knowable, to both the subscriber's telephone (for encoding) and to the cellular carrier (for decoding). Many such embodiments rely on a deterministic pseudo random number generator seeded with a datum known to both the telephone and the carrier. In simple embodiments this seed can remain constant from one call to the next (e.g. a telephone ID number). In more complex embodiments, a pseudo-one-time pad system may be used, wherein a new seed is used for each session (i.e. telephone call). In a hybrid system, the telephone and cellular carrier each have a reference noise key (e.g. 10,000 bits) from which the telephone selects a field of bits, such as 50 bits beginning at a randomly selected offset, and each uses this excerpt as the seed to generate the pseudo random data for encoding. Data

values associated with it.) Such a process steps through all 480 sparse sets of PRN data and performs corresponding dot product operations. If the dot product is positive, the corresponding bit of the auxiliary data signal is a "1;" if the dot product is negative, the corresponding bit of the auxiliary data signal is a "0." If several alignments of the auxiliary data signal within the framed composite signal are possible, this procedure is repeated at each candidate alignment, and the one yielding the highest correlation is taken as true. (Once the correct alignment is determined for a single bit of the auxiliary data signal, the alignment of all the other bits can be determined therefrom. ~~A Alignment, perhaps better known as Asynchronization,~~ **"Alignment," perhaps better known as "synchronization,"** can be achieved by primarily through the very same mechanisms which lock on and track the voice signal itself and allow for the basic functioning of the cellular unit).

Rewrite the paragraph at page 16, lines 17-19, as follows:

Security ~~of the present invention~~ depends, in large part, on security of the PRN data and/or security of the auxiliary data. In the following discussion, a few of many possible techniques for assuring the security of these data are discussed.

SB

Rewrite the paragraph extending between page 18, line 19 and page 19, line 7, as follows:

In this embodiment, a ROM in the telephone stores 256 different messages (each message may be, e.g., 128 bits in length). When the telephone is operated to initiate a call, the telephone randomly generates a number between 1 and 256, which serves as an index to these stored messages. This index is transmitted to the cell site during call set-up, allowing the central station to identify the expected message from a matching database on secure disk 52 containing the same 256 messages. (Each telephone has a different collection of messages.) (Alternatively, the carrier may randomly select the index number during call set-up and transmit it to the telephone, identifying the message to be used during that session.) In a theoretically pure world where proposed attacks to a secure system are only mathematical in nature, much of these additional layers of security might